



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier

Newsletter

N°20

OCTOBER 2010

Editorial



Dear ALCO Members, dear Readers,

By his or her role, a Compliance Officer is called upon to take an interest in many subjects, as diversified as the range of financial and para-financial activities carried on in Luxembourg. The ALCO newsletter, which is edited and coordinated by the WG 16, is becoming increasingly representative of this extension of your centres of interest.

The articles on banking secrecy and its lifting in order to defend the proprietary interests of banks, the fight against money laundering in casinos as well as the Directive (still to be finalised) on alternative investment funds (AIFMD) deal with themes that are representative of this diversity.

The roundtables which have been organised with success over the last year by the WG 34 also respond to your wish to share your experiences, questions and ideas. Those devoted to market abuse and investment fund linked life insurance products have once again demonstrated to what extent compliance solutions vary according to the business line and size of the entities involved.

The WG 33 receives ever more diverse questions. The answers are transmitted directly and the most general answers are featured in the newsletter. That is the case in this issue of the conditions of equivalence of Appointed Representatives established in the United Kingdom and the back-office processing of the day's transactions.

Newsletter

I trust that you will find this edition both interesting and useful.

Jean Noël Lequeue
President of ALCO

* *

Articles

DEFENDING THE PROPRIETARY INTERESTS OF BANKS AND BANKING SECRECY

Irrespective of the political debates on the subject of banking secrecy, this principle constitutes, in a country with a liberal system, a necessary protection of the sphere of private life and ensures the non-interference of the State in private business dealings.

From a legal point of view, banking secrecy is – despite the attacks and challenges it faces – one of the fundamental principles of Luxembourg as a financial centre, so much so that the professionals concerned consider it to be absolute (1) in nature. Moreover, the conditions for lifting banking secrecy continue to be interpreted strictly by national courts, ensuring that, if applicable, the private interests concerned are protected (2).

1. Banking secrecy: cornerstone of the financial centre

Article 41 of the amended law of 5 April 1993 on the financial sector defines banking secrecy as follows:

“All administrators, members of managing and supervisory bodies, directors, employees and other persons in the service of credit institutions, other financial sector professionals, settlement entities, central counterparties, clearing houses and foreign operators of systems authorised in Luxembourg, as referred to in Part I of this Law, shall be required to keep secret any information confided to them in the context of their professional activities. Disclosure of such information shall be punished by the penalties laid down in Article 458 of the Penal Code.

The obligation to maintain secrecy shall cease to exist where disclosure of information is authorised or required by or pursuant to any legislative provision, even where the provision in question pre-dates this law.”

In other words, banking secrecy in Luxembourg prohibits in particular managing agents, managers and employees of banks in Luxembourg from disclosing information on a bank’s clients, including in the event that the contractual relationship is terminated between a client and the bank or vis-à-vis persons with whom they may have dealings while carrying out their professional activities.

It is not possible, having regard to legislation and case law, as they currently stand in Luxembourg, to describe with certainty the nature of this secrecy: private nature, public nature or falling within the scope of the concept of the general interest.

Until such time as positive law has resolved this question, strict or liberal orientations of doctrine will continue to argue over the exact scope of banking secrecy.

On the other hand, the point on which there seems to be a consensus is that although banking secrecy is one of the cornerstones of Luxembourg as a financial centre, it cannot be considered as absolute.

Newsletter

2. Banking secrecy in Luxembourg is not absolute

As indicated in the aforementioned article 41 of the amended law of 5 April 1993, the obligation to maintain secrecy ceases when disclosure is authorised or required by or pursuant to any legislative provision; in such cases, banking secrecy may be legitimately lifted.

Other than where the lifting of banking secrecy is legally authorised, an examination of case law reveals examples, not expressly referred to in the law, where banks are released from their professional obligation of secrecy.

- At the instigation of a bank client:

Case law has confirmed a local practice which allows a client to release a bank from its secrecy obligation when the latter receives specific instructions from the client, subject to very strict conditions laid down by the SSF¹. The underlying idea is that clients “*control their secret*”², without another justification based on legislative provisions. Such a waiver by the client of the secrecy obligation is neither justified by the effects of law nor by a situation of need; it is based solely on the client’s express wish in the framework of his or her personal interests. For example, this is a situation frequently faced by banks operating on the market in Norway and Brazil, where the bank – acting as a nominee/holder of securities on behalf of a client – is required to disclose the identity of the beneficial owner in order to avoid a discriminatory tax treatment, or even penalties. In such cases, it is in the client’s interest to release the bank from its obligation of secrecy.

- At the bank’s instigation:

If the bank is involved in a dispute, the question may arise of the possibility for the bank to lift banking secrecy without the express authorisation of its client.

If a bank receives a court summons in the framework of a dispute with a client, is the bank justified, in such a case, in lifting banking secrecy in order to defend its proprietary interests?

There is very little case law in Luxembourg on this question.

We have to look to an old decision of the District Court of Luxembourg dated 26 June 1981, n° 552/81, when the Court ruled, in the framework of a dispute between a bank and one of its clients, that it was legal for a credit institution to lift banking secrecy when the bank’s proprietary interests were threatened, subject to compliance with the principle of proportionality whereby the information disclosed must be limited to the indispensable needs of the defence of the interests of the said credit institution.

The reasons adduced for this ruling indicate that “*Doctrine unanimously accepts that the bank’s legitimate interests allow it to reveal certain information. Whereas case law follows this opinion by authorising certain information to be disclosed if that is necessary in the bank’s interests*” (ruling in Tournier versus National Provincial and Unionbank).

The essential condition laid down by the court is the bank’s legitimate interest: *it is “the interest that it has to defend itself in the case of a dispute with its client”; “In this case, the bank may reveal a secret which it is normally bound to keep.”*

¹ See CSSF annual report of 2003

² Lux court 24 April 1991 P. 28, 173

The judge explained expressis verbis: “To deny the possibility for the bank to reveal secrets in the case of a dispute with its client would be to deprive it of the means to organise its own defence and expose it to a serious prejudice.”

In substance, lifting banking secrecy in the context of a dispute is legally admissible when the following conditions are all satisfied:

- the bank's proprietary interests must be called into question (the possibility of non-pecuniary damage is not sufficient);
- the secret may only be disclosed in the framework of litigation proceedings;
- disclosure must be limited to the needs of the defence of the bank's proprietary interests in accordance with the principle of proportionality.

This 1981 case law was recently invoked again. Recent cases pleaded before the courts in Luxembourg³ have concerned in particular the opposability of banking secrecy by service providers (such as registrars) acting on behalf of undertakings for collective investment (UCI) thereby authorising the latter to refuse to communicate certain contractual documents.

Although the decisions involved are summary judgements and the conclusions drawn from them must be measured, it is nevertheless important to note that the President of the District Court invoked the terms of this case law of 1981 in specifying that the lifting of banking secrecy may be necessary to enable credit institutions and financial sector professionals to exercise their rights of defence, while respecting the principle of proportionality in relation to their interests, those of the client and in accordance with the absolute nature of the secret.

These common sense solutions thus enable banks, while respecting, on the one hand, the secrets entrusted by their clients and, on the other hand, their own legitimate interests, to exercise their rights of defence thereby protecting the sphere of private life.

Karine Vilret-Huot

Lawyer and member of the Paris and Luxembourg Bar Associations

Vilret-avocats

³ Summary judgement of the President of the District Court of Luxembourg, dated 4 March 2009, in AFORGE –Sicav Luxalpha

Combating money laundering in casinos.

The history and origins of games of chance vary considerably throughout the world. The criminal roots of the casinos of Las Vegas, Russia, Eastern countries, Asia in particular with Macao, South America and Europe have not helped their reputation. Moreover, they have resulted in this sector developing in very different ways, in particular as regards its functioning and its regulation.

In Europe, the casino sector is undoubtedly now one of the most regulated and controlled sectors. The FATF recommendations transposed into European and national laws attempt to cover all the situations and threats that can exist in casinos across the world.

Casinos are by definition non-financial institutions, but they nevertheless offer similar services which make them vulnerable to money laundering risks. During a visit to a casino, customers may carry out various financial transactions, such as purchasing gambling chips, while gambling or when cashing in their gambling chips. Customers can swap currencies or purchase gambling chips or tokens with a debit card. They may also receive cheques issued in their favour or make a money transfer from or to a deposit account with a casino in the same group. All these transactions, which are carried out outside traditional financial channels, make casinos an ideal potential target for money launderers.

Casinos can also be perceived by criminals as ideal meeting places given their high-security environment protected by very effective surveillance systems, which mean that they do not have any fears for their own security. In addition, certain criminal networks see casinos as an ideal place of business since some customers may need money immediately and consequently are willing to borrow money at an exorbitant rate.

The majority of the aforementioned financial transactions are automatically excluded by European and Luxembourg laws because they are very strictly regulated and controlled almost continually by the gaming watchdog.

In comparison with other private sector activities, the application of obligations intended to prevent money laundering and terrorist financing is very closely monitored by the supervisory authorities, since casinos are often themselves very close to States and State control.

The biggest threat is the potential risk that criminal networks might succeed in obtaining the right to operate a casino via a licence or by acquiring shares in it. Attempts to control a casino or at least part of its activities are also part of this threat. In such a scenario any illegal money would simply be added to the casino's daily cash balance and declared as part of the casino's profits, generated by customer losses. In Europe, this type of scenario seems very difficult having regard to the 3rd anti-money laundering directive:

*“When registering or licensing a currency exchange office, a trust and company service provider **or a casino** nationally, competent authorities should ensure that the persons who effectively direct or will direct the business of such entities and the beneficial owners of such entities are fit and proper persons. The criteria for determining whether or not a person is fit and proper should be established in conformity with national law. As a minimum, such criteria should reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes.*

*(...) Member States shall provide that currency exchange offices and trust and company service providers shall be licensed or registered and **casinos** be licensed in order to operate their business*

Newsletter

legally. Notwithstanding future Community legislation, Member States shall provide that money transmission or remittance offices shall be licensed or registered in order to operate their business legally. Member States shall require competent authorities to refuse licensing or registration of the entities referred to in paragraph 1 if they are not satisfied that the persons who effectively direct or will direct the business of such entities or the beneficial owners of such entities are fit and proper persons”.

Article 10 (1) of the same directive also imposes an additional obligation on casinos: “*Member States shall require that all casino customers be identified and their identity verified if they purchase or exchange gambling chips with a value of 2,000 EUR or more.*” Moreover, it should be borne in mind that in Luxembourg casinos are subject to the amended law of 12 November 2004 and to the Grand-Duchy regulation of 1st February 2010 without forgetting CRF circular 20/08.

In order to limit the number of operators that might be involved in criminal affairs, the competent ministry in Luxembourg also carries out detailed, far-reaching administrative investigations to ensure that the ethics and integrity of casino concessionaries are impeccable. Licenses are only granted to candidates without a criminal record and having proven business management skills. These authorisation conditions also apply to all shareholders, bearing in mind that these requirements are the same throughout Europe.

Casino 2000 located in Mondorf is the only casino in Luxembourg and it is governed by the Grand-Duchy regulation of 12 February 1979 implementing articles 6 and 12 of the law of 20 April 1977 on the organisation of games of chance and sporting bets. In Luxembourg, as in many other countries, in order to be eligible to work in the gaming sector, employees must be approved by the Ministry of Justice.

Three other major money-laundering risks may exist in some casinos:

- cheques
- deposits
- transfers

Cheques issued by a casino are presented to the Ministry of Finance as proof of winnings and can consequently be submitted as proof of a legal income. However, the Ministry of Finance in Luxembourg does not accept cheques issued by casinos as proof of income. On the other hand, in the United States, similar documents issued by casinos exist and are accepted by the American authorities. It is important to note that in Luxembourg a cheque issued by a casino is in no way considered as proof that the amount received comes from a customer's winnings.

Some casinos in the world operate as banks and allow customers to open a deposit account. Sometimes, these deposit accounts are used to “park” money during a period of time which may or may not be determined in advance. The money laundering risk is even greater for international casino groups which accept money transfers (sometimes of money on deposit) to other countries where they operate casinos. These amounts are then transferred outside the usual financial circuit. These money transfers to the accounts of gamblers could also be declared, in the framework of a criminal network, as gambling winnings and therefore as a legal income.

As for the majority of countries in Europe, the shareholding structure of the casino in Luxembourg is scrupulously monitored. Transactions which might facilitate money laundering are refused. The casino neither authorises the opening of deposit accounts nor makes transfers to a deposit account with another casino. Moreover, it does not make transfers to customer accounts. The use of cheques is also very limited.

Newsletter

In accordance with the amended law of 12 November 2004 and the Grand-Duchy regulation of 12 February 1979, casinos have identification and vigilance obligations. All customers accessing the casino's gaming room are systematically identified and recorded. For the slot machines room, customers are identified when cashing their winnings, when exchanging gambling chips, when a cheque is issued in their favour or when they withdraw cash using a debit card.

In general, it is in their interest for casinos to know their money flows to protect themselves against tampering and to have as much financial data available as possible. In this other part of the non-financial sector, there is no shortage of money laundering scenarios. For example, the purchase and reimbursement of gambling chips in several amounts of less than approximately EUR 6,700, the receipt by casino customers of winning cheques issued in the name of third parties and the use of chips to buy goods and services or as a form of money to buy drugs.

Different cases of money laundering exist in various parts of the world involving not only casinos, gaming companies and various lotteries, but also the horse racing sector. These entities are conducive to money laundering because they handle cash.

Casinos can be used for the first phase of the money laundering process, that is to say converting the funds to be laundered from banknotes (fiduciary money) to cheques (scriptural money). In practice, the method consists in purchasing gambling chips and tokens for cash then requesting reimbursement in the form of a cheque drawn by the casino on its bank account. Another scenario consists in purchasing another gambler's chips at a higher price, thereby avoiding the need for identification at the casino's cash desk. The system can be made more opaque by using a chain of casinos which have establishments in different countries. Rather than requesting reimbursement by cheque in the same casino where the gambling chips or tokens were purchased for cash, gamblers may claim that they are planning to travel to another country where the casino has an establishment and ask for their credit to be made available in the other casino, where it will be withdrawn in the form of a cheque⁴.

Luxembourg's casino has put in place a control system which goes far beyond its legal obligations in order to minimise as far as possible the risk of money laundering. In addition, in accordance with Title IV of the Grand-Duchy Regulation of 12 February 1979 implementing articles 6 and 12 of the law of 20 April 1977 on the organisation of games of chance and sporting bets, casinos are subject to supervision and permanent control by officers of the special police service with responsibility for casino surveillance and by Customs and Excise officials designated by the Director of the Customs and Excise Department or any other civil servants designated by special decision of the Minister of Justice and the Minister of Finance.

As regards employee information, regular training sessions are organised, in particular on the main indications of money laundering. These sessions are intended to enable certain groups of gaming room employees to identify or recognise unusual behaviour. In recent years, procedures have been put in place for drawing up reports (the vast majority of which are kept and used in-house) for certain situations:

- exchanges of notes of small denomination;
- presentation of false documents;
- attempts to evade identification;
- jackpots paid in cash;
- issuance of cheques;
- presentation of counterfeit notes;

Newsletter

- attempts to exchange small denominations for large denominations, etc.

As the casino is small, it seems therefore easier for employees to detect/recognise situations where there is a risk of suspicious transactions.

Gaming companies and lotteries are also increasingly targeted by money launderers. For example, we recently noted an increase in financial transactions carried out by the same person and justified by cheques drawn on gaming organisations: lotteries, horse racing and even casinos. This shows that circuits have been put in place to organise the systematic purchase of winning tickets from legitimate holders, in exchange for the payment of an additional amount. We have also recently seen the emergence of another money laundering method in the racing and gaming sector where people actually gamble with the money to be laundered, but in such a way that they are reasonably sure to recover, at the end of the process, more or less the amount of their stake in the form of a cheque issued by the gaming or betting organisations, and corresponding to genuine gambling winnings that can be readily checked and justified. This method is far more reliable than the other one, since once they have checked the reality of the bet and winnings of the person in question, the police in charge of the investigation will in principle find it difficult to take the matter further and ascertain the origin of the money used for the initial bets.

Sundhevy Goïot
May Controls Solutions S.A.
Sundhevy.goiot@maycoso.lu

Alternative Investment Fund Managers Directive: an overview

The first draft of the Alternative Investment Fund Managers directive (AIFMD) was published by the European Commission, somehow unexpectedly, on 30 April 2009⁵.

Since then, we have seen several draft compromise proposals published by three consecutive Council Presidencies (Sweden, Spain, Belgium); two drafts AIFMD texts licensed, by the European Parliament's ECON Committee and by the Council's ECOFIN respectively; and countless industry comments, proposals and remarks.

Despite all this, there is still much uncertainty surrounding the final AIFMD text, and it is becoming more and more difficult for industry practitioners to isolate the (expected) contents of the directive from the white noise surrounding it.

In the April 2009 draft, as proposed by the European Commission, the directive contained rules for the authorisation, ongoing operation and transparency of managers of alternative investment funds (AIFMs)⁶.

However, in the AIFMD there was already much more than that, as it included provisions on funds valuation, depositary, transparency, reporting, sale and marketing, and third country (ie; non-EU) rules, for a total of 56 articles distributed on 53 pages.

The subsequent regulatory production process has failed to create a clear and straightforward text. To make a comparison, the most recent draft compromise proposal⁷ published by the Belgian Presidency of the Council contains roughly the same number of articles but is 140 pages long, including three annexes.

Why so many complexities, when dealing with a mature product such as investment funds, and what are the implications of those complexities for the compliance function?

Key AIFMD provisions

Although three official texts of the AIFMD currently exist (those licensed by the European Commission, the European Parliament and the Council respectively), for this article it is useful to refer to the last compromise proposal issued by the Belgian Presidency. This text is supposed to be reflecting the status of the recent trilogue discussions between the parties, and should constitute a solid basis for estimating how the final AIFMD text will look like.

Without entering into a full review of the AIFMD, whose text is anyway still being discussed, the following key components can be identified:

1. Authorisation and operating conditions of an AIFM

No alternative investment fund manager (AIFM) is authorised to manage one or more alternative investment funds (AIF), unless authorised. It should be noted that there is no single authorisation covering both AIFM and UCITS management company. Therefore, UCITS

⁵ Proposal for a directive of the European Parliament and of the Council on Alternative Investment Fund Managers, COM(2009)207final.

⁶ Article 1, subject matter.

⁷ Ref 14265/1/10, 4 October 2010

Newsletter

management companies already authorised will need apply to their home state regulator to be recognised also as AIFM.

Authorisation requirements for an AIFM include minimum capital requirements, good reputation and sufficient qualifications of senior management, and appropriate professional indemnity insurance amongst other requirements.

Operating conditions will impose substantial compliance costs on smaller asset management firms and boutiques, and will be similar to operating conditions imposed on UCITS management companies. An AIFM will be required to act honestly, with due skill, care and diligence in the interest of the fund and its investors. For doing so, it will have to employ effective resources and procedures, avoid conflict of interests or manage them as they arise, comply with all applicable laws and treat the investors in the fund fairly.

In order to meet these requirements, the AIFM will be expected to put in practice particular arrangements, including the following:

- In terms of remuneration practices, the AIFM is expected to have policies and practices that are consistent with the funds managed, that are consistent with sound and effective risk management and that do not encourage unjustified risk-taking.
- Proper management of conflicts is also a fundamental requirement for AIFMs. All reasonable steps should be taken to identify conflicts of interest that arise in the course of managing funds. Identified conflicts should be managed and clearly disclosed.
- A sound risk management function is to be put in place, hierarchically separate from the portfolio management. The risk management function shall implement adequate risk management systems in order to identify and measure appropriately all risks relevant to the fund's investment strategy and to which the fund can be exposed.
- Liquidity management systems and procedures will be necessary for AIFMs managing funds that are not unleveraged closed-ended ones.
- Organisational requirements for AIFMs include an obligation to use at all times adequate and appropriate human and technical resources.

The AIFMD introduces also the role of "external valuer", i.e. an entity performing the valuation of assets and the calculation of the net asset value per share/unit. The concept is widely recognised in the industry and usually referred to as "fund administrator", "central administration" or similar.

According to the AIFMD, the valuation function can be carried out either by the AIFM or by the external valuer, which should be subject to professional or regulatory registration and be able to perform the role effectively, for the concerned fund.

The role and definition of external valuer, as well as the organisation of the valuation function, has been one of the most debated elements of the AIFMD since its initial April 2009 draft, and it has been subject to a number of amendments and redrafting. One of the last compromise proposals (27 August 2010) included also a prohibition for the depositary of a fund to act as external valuer for the same fund. This prohibition has been removed in more recent texts.

- The AIFMD introduces rules on the delegation of functions from the AIFM to third parties. The functions of portfolio management and risk management cannot be delegated but to

professional parties, registered and subject to supervision. Stricter requirements apply in case of delegation to entities established in non-EU jurisdictions.

- Operating conditions refer also to the role of the depositary. Along with third country rules, this has been the most debated item of the AIFMD, and would deserve an article on its own.

In a nutshell, the AIFMD introduces a liability regime on AIF depositaries, which goes far beyond what is currently applied to UCITS depositaries. In its April 2009 wording, AIFMD introduced a completely unworkable depositary regime, whose strict reading would also have implied the impossibility for a European fund to invest into non-European securities.

The depositary liability regime has been subject to a number of amendments during the last few months – sometimes for the better, sometimes for the worse. Without entering into a too detailed analysis of the issue, it should be noted that the final regime should imply a substantially increased liability regime, including a reversal of the burden of proof (the depositary becomes responsible for assets lost, unless it can prove it has complied with the directive) with limited carve-outs and enhanced due diligence obligations in the case of appointment of subcustodians and prime brokers.

It should be noted that the European Commission is expected to amend the UCITS regime for depositaries and align it to the AIFMD regime.

2. *Transparency requirements*

Transparency requirements for AIFMs consist of: an annual report including not only the financial statements but also details on remuneration paid to senior management and staff; pre-investment detailed investor disclosures (including, for instance, the circumstances under which a fund may use leverage, the types and sources of leverage permitted and the associated risks, any restrictions to use of leverage and of any collateral and asset re-use arrangements); and finally, detailed regulatory reporting.

3. *Rules applicable to specific types of AIFs*

The AIFMD provides for additional obligations for managers of leveraged funds and for managers of private equity funds.

In the case of leveraged funds, the AIFMD imposes additional vigilance obligations on competent regulatory authorities, as well as on the ESMA⁸, which have to assess the extent to which the use of leverage contributes to the build-up of systemic risk. As far as AIFMs are concerned, those must demonstrate that the leverage limits for each fund they manage are reasonable and that they comply at all times with the limits imposed by law or fund's rules.

Rules applicable to private equity funds are still a matter of debate. Although older versions of the AIFMD included rules in terms of acquisition of non-listed companies, the latest drafts are incomplete and refer to ongoing dialogue discussions. We may need some more time to have more clarity on the matter.

4. *Passporting rights*

One of the key features of the AIFMD is undoubtedly that it establishes passporting rights for AIFMs and for the funds they manage. Those passporting rights are not so different from those currently applicable under the UCITS IV regime. It should be noted however, that unlike

⁸ The newly established European Securities Market Authority

Newsletter

UCITS, passporting rights for AIFs apply only in the case of marketing to professional investors.

This does not mean that AIFs cannot be sold to retail investors. EU Member States may allow the sale of an AIF also to retail investors, but can impose additional or stricter requirements on the AIFM or on the product.

5. *Third country rules*

Third country rules have been, along with depositary rules, the most debated part of the AIFMD and probably the only reason why no final text has yet been licensed.

In a nutshell, the key issue with third country rules is how to reconcile the Council's view with the view of the European Parliament, as expressed in their respective official proposals.

The most obvious difference between the European Parliament's text and the Council's text is that according to the former, non-EU-domiciled funds may, under certain conditions, be granted a European marketing passport while according to the latter, no passport is made available and the decision to allow marketing rests on each Member State, separately.

More specifically, the European Parliament's approach is that funds that are non-EU-domiciled may market their units or shares in any Member State, as long as they are domiciled in a qualifying country (specific criteria are established, focusing mainly on exchange of information and cooperation mechanisms with Member States).

If the non-EU fund is managed by a non-EU AIFM, enhanced criteria apply and the country where the AIFM is domiciled must also qualify. Additionally, it introduces rules for investment into non-EU-domiciled funds (in addition to marketing rules) to avoid circumventing marketing rules via private placement arrangements. Substantially, institutional investors that are EU-domiciled cannot invest into non-EU funds unless those funds are established in qualifying countries.

The Council's text instead makes a clear distinction between those funds managed by an EU-domiciled AIFM and those that are not.

If the fund is managed by an EU-domiciled AIFM, marketing may be granted under the conditions that the AIFM complies with the requirements of the AIFMD (with the exception of depositary rules) and that cooperation arrangements exist between the Member State where the AIFM is domiciled and the supervisory authority of the third country where the fund is domiciled.

If the fund is managed by a non-EU-domiciled AIFM, the AIFM must comply with transparency, reporting and disclosure rules. Cooperation arrangements between the Member State where the fund is marketed and the supervisory authority where the AIFM is domiciled must include rules for the oversight of systemic risk in line with international standards.

In terms of delegation of service provisions to providers established outside the EU, the Council's and the European Parliament's text differ greatly. While the Council's text is silent (or better, deletes any relevant provisions as contained in the original EC AIFMD draft), the European Parliament's text contains provisions that apply to the delegation of activities such as administrative tasks and valuation of assets to a non-EU entity.

The 4 October compromise proposal is the latest attempt to make clarity on the matter. But there is little point in providing here a detailed analysis – this is definitely work in progress, still being discussed in trialogue.

6. *Competent authorities*

AIFMD is naturally aligned to the new EU supervisory framework, therefore requiring increased cooperation and coordination between national regulatory authorities and ESMA – including processes for imposing administrative penalties, right of appeal against those, and dispute settlement procedures.

New challenges for the compliance function?

The challenges introduced by the AIFMD for the compliance function can be seen from three angles: from a rule-making process angle, from a product design/management angle, and from a pure compliance oversight function angle.

In terms of rule-making process, the most challenging activity for the past two years has been to keep up to date with regulatory discussions at European level, trying to make clarity out of the several, and most often contradictory, AIFMD texts.

One can only hope that the recently approved financial supervision reform, with the establishment of ESMA, will substantially improve and streamline the fund regulatory production process.

As the regulatory making process becomes more and more centralised at European level (a trend which we have seen increasing in the last 5-6 years), the compliance function will be required to stretch outside of its national borders, to ensure that it is aware of regulatory initiatives well before they are implemented in national laws. From this point of view, national industry associations, such as for Luxembourg ALFI, ABBL and the same ALCO, will play a key role and will need making additional efforts to ensure their voice reaches out to Paris (in the case of ESMA).

In terms of product design and management, from a Luxembourg point of view, challenges should be limited. The legal and regulatory framework of the Grand-Duchy is broadly in line with most of the AIFMD requirements, although fine tuning will be required. The SIF law provides for a very solid basis to build upon.

However, attention will have to be paid to depositary provisions (in particular, with reference to the depositary-prime broker relationship) and on the external valuer provisions, in particular should the final AIFMD text impose a legal (and not only functional) segregation with the depositary.

Enhanced due diligence obligations will impose additional efforts also on the compliance function, that will be called upon either to perform reviews of sub-custodians and prime brokers, or to ensure that appropriate due diligence is employed by the business when selecting them.

In terms of compliance oversight, again for a mature regulatory environment such as Luxembourg organisational requirements imposed on AIFMs should not provide particular concerns. However areas such as remuneration practices and transparency and reporting requirements, in particular for private equity business, could be demanding at least in the initial stage, before a solid business practice is established.

Conclusions

The final word on the AIFMD has still to be written. Since the beginning of the Belgian Presidency (but also before) a number of revised compromise proposals have been circulated to the industry, including sometimes significant changes – although the basis structure of the directive has remained pretty much the same since August 2010.

The last official position, at the date of writing, is that the AIFMD should be licensed by the European Parliament in plenary vote on 18 October, even if rumours are that a vote is more likely to happen in November. As the vote will be held only on the basis that trialogue discussions have finally reached an agreement, the vote would imply green light for the AIFMD. Level 2 measures will then be produced.

Newsletter

Almost at the same time, we should also see the much rumoured UCITS V directive (or UCITS IV ½ as some European Commission officers informally name it), that will introduce almost surely depositary liability standard comparable to (or even stricter than) those included in the AIFMD.

Stefano Pierantozzi
Head of EMEA Fiduciary Oversight & Research
Citibank International

Round Tables

One year ago the round table lunch meetings were launched. Already 80 participants have accepted to share their experience, their questions and their feelings on 5 different topics⁹. Although it is not easy to go through tricky issues in only 100 minutes, most of the participants agreed to take the opportunity to start interesting peer to peer discussions around the table.

MARKET ABUSE - prevention & detection

For this first meeting of 2010 we decided to focus on the prevention and the detection of market abuse. More than 30 members showed interest, but only 16 of them were available to attend on the 24th.

14 completed questionnaires have been collected. Their summary is hereto attached.

This time, we were glad of having Cyril Mathieu as expert to enhance the discussions.

Cyril Mathieu is Assistant Manager Fund Compliance at HSBC. He has participated to ABBL working groups and, subject to ALCO members' interest he is willing to re-launch the ALCO Market Abuse working group. He is chairing to discuss further this interesting matter and share practice. Don't hesitate to join this working group, if you are interested in the subject.



- He introduced the meeting by commenting some slides¹⁰ explaining the specificities & evolutions of the subject. He also questioned how the Market Abuse Directive might be reviewed soon as there is an obvious hardening of public and regulators attitudes to improve market cleanliness and integrity. Finally, he highlighted some best practices expected to reinforce the prevention of market abuse.
- A few slides showed a sample of the market abuse cases that have been commented in the newspapers:

⁹ (a) expectations of new members towards ALCO ; (b) MIFID – suitability ; (c) Compliance & Risk Management – links in the fund industry ; (d) AML Filtering (e) Market Abuse –detection & prevention

¹⁰ The PowerPoint presentation is available upon request.

Newsletter

- The GBP 1,7 million FSA fine levied against Shell Petroleum in 2004 and the USD 120 million settlement agreed by the company with the SEC.
- The GBP 25K FSA fine against the director of Cambian Mining in 2005 and the GBP 59K fined by the FSA against the director of Byron Holdings in 2009.
- The sentenced use of insider information by a dentist who had been informed by his son who could get insider information during a student job with a broker (2009).
- Several persons sentenced to jail for insider trading in Hong Kong in 2009; several criminal prosecutions by the FSA since 2008.

The discussions were moderated (& stimulated!) by Pierre Hennericy and Charles van Doorslaer was in charge of summarizing the discussions.



Once again the questionnaires showed a wide range of practices¹¹. The diversity of the answers can be explained partially by the kind of business (banking, insurance, asset management...) as well as by the size of the companies. Belonging or not to an international group, being listed or not on a stock exchange is even more determining for the prevention & controls put in place and for the level of awareness.

It is important to keep in mind that the ideas expressed in the questionnaire, the discussions and this summary are not reflecting any position, nor from the ALCO, nor from any institution of which a member has participated. Although it is difficult to reflect all the details of the discussions in a written summary, this document aims at reflecting the extent of the talks we had during the session.

Prevention:

There isn't one single way to organise prevention. Different complementary ways might be used.

A compliance officer might organise trainings. These trainings can be given through e-learning or face to face sessions or a combination of both. Some companies benefit from training materials made available by a foreign parent company, some organise it themselves. External trainers can be hired and exposed employees can also participate to seminars & conferences.

Some banks train all employees upon their arrival. Others launch specific training sessions focused on certain departments. Most of the participants have already tested e-learning or expect to start e-learning sessions in a close future.

¹¹ It has to be noted that 14 completed questionnaires cannot be considered as a representative number compared to the hundreds of financial companies that are present in Luxembourg.

Newsletter

Everybody agrees training should be as close as possible to the daily activities of the trainees. It is a big advantage when a trainer has gained experience in the same business and can illustrate concepts with his own experience and anecdotes.

Awareness can also be improved when compliance officers participate to business meetings, especially when these take place on a regular basis. And if they don't get invited to these meetings, they invite themselves!

Quite some documents are issued to inform employees about their responsibilities & duties.

- An internal **code of conduct** applies to all employees.
- When the company is listed, a **dealing code** has to be agreed by any potential insider within the company. Blocking periods and specific procedures need to be respected strictly.
- All employees linked to asset management activities need to comply with specific rules on employees **personal transactions**.
 - o Some companies are asking all concerned employees to notify immediately all their transactions in securities handled through another bank. Results are mitigated. Depending on the way the rules have been implemented¹² and the level of awareness of the employees, few or many operations are reported. It is almost impossible to control the exhaustiveness. An employee may report a lot of transactions, but it might be that he will not report a transaction that he might consider himself as a forbidden insider deal.
 - o Some banks request from their employees to buy & sell securities exclusively through their account at the bank. Success may be depending on the tariffs that are offered to employees. There again, it doesn't prevent an employee to also execute some insider trades in a different institution. A pre-trade clearing by compliance might offer a solution.
 - o Specific constraints can be issued about a minimum delay between acquisition and sales (E.g. minimum 3 days, 10 days...), a maximum number of transactions per month etc.
 - o To avoid conflicts of interests or difficulties in monitoring, investment in 'own' products might be forbidden.
 - o In certain countries (E.g. France, UK) bank statements are sent in copy to the employer.
 - o It also happens that employees are asked not to invest in any securities, unless it is through discretionary management or in UCITS. Sometimes they are asked to invest only through a dedicated investment company or to have each investment decision first validated by the compliance officer before being executed.

Are awareness messages helpful? It's important to target the right persons and to have very short texts. It might be interesting to check, through a acknowledgment of receipt, how many messages are opened and to have some statistics about the received feed back. When people are asked to do something (e.g. print a form that they have to sign & return), this will encourage them to have a closer look to keep in mind what it is about.

Are Chinese walls helpful? Avoiding employees getting access to certain data, certain files, certain departments is essential in a lot of companies. Especially when one is offering investment banking, corporate finance as well as private banking or retail services, one needs to make sure that information is not circulating easily from one place to the other within the organisation.

Should compliance officers have permanent access to all the activities? Not necessarily a permanent access, but they need to have the possibility to obtain access on request. If access is refused, the compliance officer should escalate the issue to the board, who will then determine how the access will be organised.

Commitment of senior management is probably the main key to success.

64% feel senior management have a sufficient understanding of the Market Abuse risks. A way to check awareness of Senior Management is observing how they react when they are notified of an

¹² Through e-mail or handed over personally, requesting or not a duly signed notice of receipt, combined or not with a training session....

Newsletter

information request from the Authorities. The question of the awareness should not be measured through the level of *understanding* but rather through the level of *support* senior management grants to prevent and to fight against market abuse. Can one compare the level of support against M.A. with the level of support for A.M.L.?

Commitment significantly depends on the manager's experience and working environment. It seems that managers who are linked to UK, USA, France, and Far East ... have often a much higher level of awareness than those who are linked to Belgium, Switzerland or Eastern Europe ... The influence of the mother company is of course determinant as well.

How to draft a Market Abuse Policy, a code of conduct? Most of the participating companies have drafted their Policy on their own or have received a standard text from their parent company. Most of them include examples of information, circumstances, events that should be considered as inside information, a procedure for escalation, an obligation to report any inside information leak and rules to handle such leak and even rules about trading in clients' financial instruments...

Most of participants have a list of permanent insiders. Some of them (36%) have also had specific insiders' lists related to certain projects

64 % confirm that they already have mapped sources and typical flows of inside information. Same number is trying to identify all clients that are to be flagged. Flagging potential insiders (or potential market manipulators) needs to be done through the client due diligence as from the entry into relationship.

Detection

Which are our main obligations concerning detection? Identify persons closely related to listed companies - identify them among clients & employees, detect suspicious transactions (insider trading and market abuse) and monitor employee transactions.

Flagged clients and employees are often gathered together on a watch list used for specific controls.

A few participants (29%) have developed a proactive system to get alerts on transactions or market events enabling a priori detection. Half of the participants have a posteriori detection systems.

Among all the transactions that are expected to be detected by the systems, insider trading and fictive orders are the most inclined to be highlighted (46 %). They are followed by 'pump & dump - trash & cash' transactions (29%) and then by front running and market timing (both 21%).

When one cannot reckon on a performing automated tool that helps to detect insider trading or market manipulation, is it efficient to focus the controls on traders? Often traders know the rules very well. Sometimes they contact compliance in a proactive way. Most alerts on transactions from traders require deep analysis, but the outcome of the analysis is rarely positive.

It is possible to perform ex post detection in an efficient way through queries built with general software like Business Object, Access or even Excel, generating automated daily reports. Here consideration should be given to the accuracy and efficiency of the whole detection process with regard to external auditors and prudential authorities.

In 71% of the answers, there is a group policy regarding market abuse, but in only 57% of the cases detection and monitoring of market abuse is coordinated within the group, with some controls delegated to the company.

Another issue is about the difficult balance between the need of escalating the suspicious transactions to a parent company on the one hand and the bank secrecy & no tipping off principles on the other hand.

Newsletter

Expectations from the authorities

Only one participant seems to have received feed back from the authorities on the reporting of a suspicious transaction. Does this mean that CSSF or FIU require discretion that is even higher than for AML issues? Or do enquiries take a lot of time to conclude? Or that there is no feed-back from the investigating foreign authorities? It's difficult to determine. Prevention and detection of market abuse is not an obligation of results but of means. The risk of having an authority blaming you that “you should have known” or “you should have detected earlier” is not easy to evaluate.

Consequently, it might be a good suggestion to document as much as possible why the bank decides, on a risk-based approach, not to monitor certain categories of transactions or of accounts.



Conclusion

We feel that most of the participants have appreciated the opportunity of asking their questions, sharing experience and exchanging thoughts. Some of them have showed interest in reactivating and joining the Working Group on Market Abuse to continue the brainstorming and some other to join the Working Group organising the Round Table discussions.

© Working Group 34 “Round Tables”¹³

¹³ Charles van Doorslaer, Pierre Hennericy, Xavier Leydier, Vincent Salzinger, Mike Sommer, Eef Liesens, Jean-Michel Righi

Newsletter

Summary of the answers received to the questionnaire

Bank	AM	Fund	Insurance	Other	Total
11	1	0	1	1	14
79%	7%	0%	7%	7%	100%

ALCO Round Table nr 4 Prevention & Detection of Market Abuse - Preliminary questionnaire

Prevention – Training – awareness: what's included in your company prevention?

- code of conduct, dealing code, policies - to all/to exposed employees only
- training: internal - to all/to exposed only
- training: external - to all/to exposed employees only
- awareness messages (by e-mail...) - to all/to exposed employees only.....
- chinese walls: on physical access?
- and on IT access?

Commitment of senior management

- Do you feel your senior management has a sufficient understanding of the risks they face?
- Have responsibilities, duties & ownership been determined at all levels?

Prevention of (external & internal Insider) trading -

- Have you mapped sources and typical flows of inside information?
- Does your insider policy include:
 - examples of information, circumstances, events... that should be considered as inside information
 - a procedure for escalation of information about events that may constitute inside information
 - an obligation to report any inside information leak & rules to handle such leak
 - rules re: trading in clients' financial instruments to all or certain members of the staff
- Have you got, at some stage, some external support from law firms/consultants?
- Are your clients identified or screened in some way in order to be flagged as potential insiders?

About (internal) insiders lists (re: employees, management)

- Have you a list of permanent insiders (structured by functional responsibility/exposure)?
- Have you ever had a „project-specific“ insiders list structured by inside information item or project?

If your bank is member of an (international) banking group:

- Is there a Group policy regarding market abuse
- Is detection /monitoring coordinated within the group
- Are control processes delegated to your entity

Personal account dealing regime / policy on personal employee transactions

- Are certain managers/employees to obtain prior permission to trade (pre-trade clearance)?
- Have managers/employees to respect trading black-out periods?
 - permanent trading prohibition?
- Are employees required to report a posteriori security transactions made on external accounts?
- Do your employees and managers ask for clearance as a matter of practice on their own initiative?
- Do you restrict trading "channels" (e.g. dedicated investment firms) of managers/employees/?
- Are certain managers/employees required to declare certain of their holdings?

Detection: what kind of systems do you use?

- a proactive system to get alerts on transactions or market events or a priori detection?
- a passive database of transactions to be analysed or a posteriori detection?
- a transaction monitoring system that has been developed internally?
- a transaction monitoring system that has been developed by an external service provider?

Examples of transactions that you expect to be detected by your institution:

- insider trading
- front running
- market timing
- late trading
- pump & dump / trash & cash
- concentrations of unusual operations
- fictive orders

Which kind of market abuse has your institution already detected?

None: 6
Insider dealing: 5
Front running: 2
Other: 1

YES	%	NO	%	All	%	Exposed	%
14	100%		0%	12	86%	1	7%
9	64%	5	36%	4	29%	4	29%
3	21%	6	43%		0%	1	7%
8	57%	6	43%	3	21%	3	21%
12	86%	2	14%		0%		0%
13	93%	1	7%		0%		0%
YES	%	NO	%	No opinion	%		
9	64%	1	7%	4	29%		
9	64%	3	21%	2	14%		
YES	%	NO	%	N/A	%		
9	64%	4	29%	1	7%		
11	79%	2	14%	1	7%		
11	79%	2	14%	1	7%		
10	71%	3	21%	1	7%		
9	64%	4	29%	1	7%		
1	7%	12	86%	1	7%		
9	64%	4	29%	1	7%		
YES	%	NO	%	N/A	%		
10	71%	3	21%	1	7%		
5	36%	8	57%	1	7%		
YES	%	NO	%				
10	71%	4	29%				
8	57%	6	43%				
8	57%	6	43%				
YES	%	NO	%				
6	43%	8	57%				
9	64%	5	36%				
8	57%	6	43%				
9	64%	5	36%				
7	50%	7	50%				
4	29%	10	71%				
9	64%	5	36%				
YES	%	NO	%				
4	29%	10	71%				
7	50%	7	50%				
5	36%	9	64%				
1	7%	13	93%				
manual	%	semi-automatic	%	N.A.	%	no answer	%
6	43%	2	14%	2	14%	4	29%
3	21%	2	14%	5	36%	4	29%
3	21%	2	14%	5	36%	4	29%
2	14%	4	29%	4	29%	4	29%
4	29%	3	21%	5	36%	2	14%
6	43%	0	0%	2	14%	6	43%
6	43%	0	0%	4	29%	4	29%

Round table of 3 May 2010

Insurance: CAA Circular Letter 08/1 on investment rules for life insurance products linked to investment funds

Present: 16 ALCO members

Technical Advisers:

- Nicolas Limbourg, VITIS LIFE SA
- Thierry Flamand, PwC

For WG 34:

- Pierre Hennericy, Banque Pictet & Cie, Moderator
- Xavier Leydier, Banque Havilland SA, Secretary
- Eef Liesens, VITIS LIFE SA, Initiator of the roundtable
- Charles van Doorslaer, KBL EPB, organiser

Introduction

This “insurance” roundtable was organised at an opportune time since, following the financial crisis, there is clearly a greater awareness within the profession regarding certain risks which were previously underestimated. These risks concern both the Custodian banks and the underlying assets. Although some progress was made in 2009, there has been a real step forward in 2010 insofar as more and more insurance companies are putting in place tools to improve underlying risk controls as regards the management of the invested assets. We wish to thank in particular Eef Liesens, who initiated this roundtable, as well as Nicolas Limbourg and Thierry Flamand for their expertise and their contributions, as technical advisers, to the discussions.

Roundtable and discussions

The discussion was launched on the basis of a set of seven questions transmitted to participants in advance (see annex).

The participants unanimously recognised that the procedures for opening and managing bank accounts are not sufficiently adapted to the funds linked to life insurance policies.

Most of the companies represented have put in place, or have plans to do so, a database containing all the financial data of the custodian banks. They are all facing the same major problem, namely that of the data feeding of such databases, for several reasons:

- the lack of electronic data transmission methods, which means that data has to be input manually;
- the same assets with different custodian banks can be included with different values or a different classification;
- the NAV level according to “side-pocketing” which depends on the insurance company’s choice.

The participants regretted a lack of communication by the Insurance Regulator, the Commissariat Aux Assurances (CAA), in particular at the time of the most recent crises (Madoff, 2009 – Greece & Portugal in April 2010).

The roundtable revealed that:

- Some participants do not have (yet) any databases.
Consequently, controls are carried out manually, line by line, on an a posteriori basis. Few companies have developed (or finalised) online controls. In general, the activities of custodian banks and those of insurance companies are clearly separated.

Newsletter

Each transaction is subject to a priori controls and a posteriori controls are carried out on a monthly basis.

- Although some reporting tools are available commercially, some insurance companies have opted to develop their own customised in-house database.
 - Participants are faced with a constant problem, namely the valuation of unlisted securities.
 - Reporting can be carried out on the basis of the reports transmitted by the custodian bank.
 - The custodian bank's reports can also be substantiated by the valuations received via an internationally recognised valuation system, such as, for instance, Bloomberg, Reuters or Telekurz.
 - Some participants are not as advanced as the others when it comes to the control of investment restrictions.

It was noted that:

- Few custodian banks control the management and the allocation of assets in the insurance portfolio.
- Insurance companies are faced with the problem of putting in place international financial reporting standards (IFRS).
- In addition, they are faced with the problem of managing assets subject to three different circulars dating from 1995, 2006 and 2008 and which are superfluous to some extent, thereby creating a problem of "educating" partners.
- Controls are centralised, even if different sub-custodian banks or managers exist in different countries.
- Some insurance companies work with several external managers and only one centralised custodian bank. In such cases, any breaches are reported directly to the external managers. Some companies recommend that a certification of the knowledge of the CAA rules should be included among the terms and conditions of the management mandate. However, the participants agreed that managers have a contractual obligation of means and not of results.
- There is a grey area as regards the placing of orders for the custodian bank: from whom should it receive instructions? The managers may place orders in different ways at their choosing: either directly with the custodian bank or via the insurance company.
- There is as well the problem of a client's intervention in the change in the overall strategy or for a specific investment, whether vis-à-vis the insurance company or directly with the custodian bank. In order to avoid the insurance policy being reclassified, some participants stressed that they prohibit asset managers from placing orders on the basis of client instructions. Asset managers must comply with discretionary management rules.
- The participants recognised the shortcomings of agreements on the attitude to adopt in the event of breaches. As a general rule, the participants recognised that management agreements lay down the rules between the parties and impose on each party an obligation of means. The participants acknowledged that they are often faced with the problem of the transposition by custodian banks of the investment grids produced by insurance companies, in order to adapt them to their internal grid. This results in analytical difficulties for the insurance companies.
- Most of the companies represented have the same problem of getting rid of "undesirable" assets when they take over a portfolio. This problem arises mainly when accounts invested in insurance products are transferred or when an existing bank portfolio is converted to a life insurance policy when an account is closed. A life insurance company can sometimes receive a series of assets which are not authorised by the CAA. The participants acknowledged that in such a case it is a problem for the insured party. In general insurance companies adapt their investment strategy according to the liquidity of the received securities, if applicable. They

Newsletter

may, request the insured party to sign an indemnity letter in order to transfer the ineligible securities or to set out the details of a disposal strategy for the securities in question, if they are illiquid or unsalable.

- As well, insurance companies are faced with the difficulty of the certification of investment given the diversity of financial products. Consequently, is the decision regarding the eligibility of an investment the responsibility of the custodian bank or of the manager?
- Portfolio controls can be prioritised according to a risk-based approach, starting with the biggest portfolios or by the most non-compliant external managers or the biggest external managers, etc.
- For banks which provide both “fund” services and “insurance” services, the “insurance” related controls are generally carried out by the “Fund Compliance” entity.

As regards to domiciliation, the meeting revealed that most of the participants are sometimes faced with a certain amount of confusion between the roles of domiciliary companies, custodian banks, managers and insurance companies. Different approaches are adopted in order to determine these roles more precisely:

- Responsibility for monitoring the investment limits may be entrusted to the company’s “Fund” department.
- The “NAV” of the insurance product remains dependent on the NAV produced by the custodian bank.
- As custodian banks are supervised by the CSSF and not the CAA, banks are often not fully familiar with the particularities of the CAA.
- Insurance companies often consider that their role entails responsibility for “second level” controls.

As regards to Due Diligence checks for selecting Asset Managers:

- Most participants require Asset Managers to be qualified in their country of residence. This requirement is supplemented by a Due diligence check. Some participants consider that the selection should be subject to the decision of an acceptance committee, while others consider that neither standard formalities nor an acceptance committee are necessary, since every new Asset Manager must be accepted by the management.
- The definition of qualification poses a problem for the participants since, although in Luxembourg the system seems to be fully regulated (if the intermediary is not supervised by the CAA, FSP are supervised by the CSSF), this is not the case in foreign countries, where the notion of supervision by a regulator does not always exist. In addition, according to the CAA directives, there is an issue with the responsibility of the counterparty if due diligence searches are not carried out.

The participants then review the problem of claims in the event of the disappearance of assets or in the event of a substantial loss. It emerged from the discussions that all the participants agree that the responsibility lies with the insurance company, as the custodian bank acts only as a “nominee”. In addition, for custodian banks there is the problem of the identity of the shareholder and contact with the latter, as well as the problem of accessing to information concerning the latter. In any event, the participants strongly recommended greater proactive cooperation prior to any dispute:

- For some participants, this cooperation involves monthly or quarterly meetings with the managers, but not with the custodian bank.
- For others, it involves case-by-case analyses via the custodian bank.

Newsletter

- The controls carried out to check the level of investments are in general “polluted” at several levels by inherent problems due to the level of activity, such as the multiplicity of contacts, securities, types of NAV, NAV frequency, etc.
- As regards to their levels of controls, the participants recognised that although major operators perform external controls, smaller operators find it difficult to set up such controls or to impose their controls.
- Finally, the participants regretted their dependence on information transmitted by custodian banks and questioned the possibility for them to correctly assess such information.

Conclusion

This roundtable revealed once again the diversity of the Compliance Officer’s role. This diversity depends on the entity within which the Compliance Officer operates. This is particularly true in the area of insurance. It involves in fact different types of operators in Luxembourg. It would be beneficial for the financial Sector as a whole that further improvements in the coordination between the two supervisory bodies, namely the CAA and the CSSF, are made in order to optimise a regulatory harmonisation and therefore the levels of controls.

Participants can refer to the Association of Insurance Companies (ACA) which issues recommendations.

The roundtable participants appreciated the opportunity to compare their points of view and share their interpretations and ideas for solutions, as well as the benchmarking opportunities that this kind of exercise offers each participant as regards to professional practices in Luxembourg.

For WG 34, Xavier Leydier

Member's Question

Question: *Can Appointed Representatives established in the UK be considered as equivalent to FSP under the laws of Luxembourg vis-à-vis which parties subject to the LAB/CFT rules in Luxembourg can benefit from an identification exemption?*

Answer:

This question concerning *Appointed Representatives* (herein “AR”) is not so much important from the point of view of their personal status but rather as regards the treatment of their own clients, in particular in the case of the distribution of financial products (shares in funds, insurance products, etc.).

In general, an AR is a natural person or a legal entity that is registered with the Financial Services Authority and is supervised by a “Principal” that acts as sponsor. A contractual relationship must exist between the AR and the principal; the latter must moreover be an entity that is “authorised” by the FSA. The status and remit of the AR are specified in section 39 of the Financial Services and Market Act, 2000.

However, an AR is not regulated and is not necessarily subject to the obligations regarding the prevention of money laundering and terrorist financing activities. Consequently, in accordance with the risk approach principle, only the implementation of a series of due diligence measures will make it possible to distinguish ARs that can be considered as equivalent to FSP in Luxembourg from those that cannot.

The following points would seem to require special attention:

- ensure that the AR is listed in the FSA register (available on the Internet);
- establish the relationship between the Principal and the AR: this involves checking, via supporting documents (copies of contract, agreement, etc.), that there is a valid contractual and operational relationship between the two parties as well the attribution of obligations and responsibilities with regard to the LAB/CFT rules. You should then check the existence and conformity of the service or product in question with regard to the scope of activities entrusted to the AR by the Principal;
- check the reliability of the Principal (status, regulation, reputation, etc.) by all valid means;
- establish in concrete terms the control exercised by the Principal over the AR: it would seem to be indispensable in particular to obtain a guarantee from the Principal in respect of the AR (AML Letter by which the Principal confirms that it requires the AR to apply the LAB/CFT obligations as provided for in the 3rd EU anti-money laundering directive, confirming that the AR has not been suspended or had his authorisation withdrawn, that he does not have any convictions or professional sanctions and that he has not been involved in any criminal affairs, etc.).

These due diligence measures should be applied not only when the relationship is established but also throughout the relationship.

Newsletter

Thus, the principle of equivalence can only be considered as acceptable if the following two conditions are satisfied:

- that the Luxembourg FSP is satisfied once these due diligence checks have been carried out;
- that financial or similar flows (e.g. subscription orders) are duly transmitted by the AR in question and do not come directly from third parties (e.g. investors). Otherwise, i.e. if the flows are received directly by the Luxembourg FSP and not via the AR, it is advisable to obtain an undertaking from the AR regarding the identity of the end client/investor or to apply the principle of full identification to the latter.

The last requirement is essential. In any event, an AR that has the simple status of an intermediary or a business introducer, without playing any subsequent part in the execution of the transactions made by the end client/investor, cannot be considered as equivalent to a Luxembourg FSP. In such a case, both the AR and the end client/investor should be identified. Thus, for reasons of operational efficiency, the identification system to be applied to an AR and/or the end client/investor may be determined at the time the relationship is established.

For more information, please refer to section 12 of the FSA “AR Handbook” available on the Internet.

Vie associative

VIE ASSOCIATIVE

GROUPES DE TRAVAIL ACTUELS

Groupe de travail 11

Site Internet

Responsable Olivier GILSON
Téléphone +352 48 48 80 51 08
olivier.gilson@efa.eu

Groupe de travail 16

Commission permanente juridique et relations publiques

Responsables Claudine FRUTSAERT
Téléphone +352 44 24 24 43 15
claudine.frutsaert@axa.lu

Jean-Marie LEGENDRE
Téléphone +352 24 67 26 07
Jean-Marie.LEGENDRE@ca-luxembourg.com

Groupe de travail 20

Funds practices and recommendations AML

Responsable Patrick Watelet
Téléphone +352 45-14-14-231
patrick.watelet@citi.com

Groupe de travail 21

Interprétation pratique des restrictions d'investissements de fonds

Responsable Tim WINFIELD
Téléphone +352 34 10 23 85
tim.winfield@jpmorgan.com

Groupe de travail 27

Formations IFBL

Coordinateur Sundhevy GOÏOT
Téléphone +352 621 30 23 63
sundhevy.goiot@maycoso.lu

Groupe de travail 29

Abus de marché

Coordinateur Cyril MATHIEU
Téléphone +352 40 46 46 400
cyrilmathieu@lu.hsbc.com

Groupe de travail 30

Domiciliation de société

Coordinateur Sophie RASE
Téléphone +352 40 25 05 408
sophie.rase@maitlandgroup.com

Coordinateur Marie-Hélène CLAUDE
Téléphone +352 48 18 28 39 03
marie-helene.claude@alterdomus.lu

ASSOCIATION ACTIVITIES

CURRENT WORKING GROUPS

Working group 11

Website

Owner Olivier GILSON
Phone +352 48 48 80 51 08
olivier.gilson@efa.eu

Working group 16

Legal and public relations

Owners Claudine FRUTSAERT
Phone +352 44 24 24 43 15
claudine.frutsaert@axa.lu

Jean-Marie LEGENDRE
Phone +352 24 67 26 07
Jean-Marie.LEGENDRE@ca-luxembourg.com

Working group 20

Funds practices and recommendations AML

Owner Patrick Watelet
Phone +352 45-14-14-231
patrick.watelet@citi.com

Working group 21

Practical interpretation of fund investment restrictions

Owner Tim WINFIELD
Phone +352 34 10 23 85
tim.winfield@jpmorgan.com

Working group 27

Training IFBL

Coordinator Sundhevy GOÏOT
Phone +352 621 30 23 63
sundhevy.goiot@maycoso.lu

Working group 29

Market abuse

Coordinator Cyril MATHIEU
Phone +352 40 46 46 400
cyrilmathieu@lu.hsbc.com

Working group 30

Domiciliary agent

Coordinator Sophie RASE
Phone +352 40 25 05 408
sophie.rase@maitlandgroup.com

Coordinateur Marie-Hélène CLAUDE
Téléphone +352 48 18 28 39 03
marie-helene.claude@alterdomus.lu

Newsletter

Groupe de travail 33

Réponses aux questions des membres

Coordinateur Carine VAN MULDER
Téléphone +352 47 97 28 15797 2815
CARINE.VAN-MULDER@kbl-bank.com

Working group 33

Answers to questions of members

Coordinator Vincent WILLEM
Phone +352 49 924 3956
CARINE.VAN-MULDER@kbl-bank.com

Groupe de travail 34

Tables rondes

Coordinateur Charles VAN DOORSLAER
Téléphone +352 47 97 39 09
charles.van-doorslaer@kbl-bank.com

Working group 34

Round tables

Coordinator Charles VAN DOORSLAER
Phone +352 47 97 39 09
charles.van-doorslaer@kbl-bank.com

Groupe de travail 35

Doctrine

Coordinateur Guillaume BEGUE
Téléphone +352 26 96 22 31
guillaume.begue@bnpparibas.com

Working group 35

Doctrine

Coordinator Guillaume BEGUE
Phone +352 26 96 22 31
guillaume.begue@bnpparibas.com

MEMBRES ET VIE ASSOCIATIVE

MEMBERS AND ASSOCIATION ACTIVITIES

Nombre de membres (au 30/09/2010):

Banques	222
Fonds	93
Fonds / Banques	28
Assurances	58
Consultants / Réviseurs	35
Admin. et domiciliation de sociétés	17
Avocats	8
PSF	48
Gestion de fortune	22
Autres	14
Effectif total:	545

Membres effectifs 440
Membres d'honneur 105

Effectif total: 545

Réunions et activités:

Mensuellement	Réunions du conseil d'administration
1 / 2 x par an	Réunions plénières
2 / 3 x par an	Rencontres informelles autour d'un thème

Number of members (as per 30/09/2010):

Banking sector	222
Funds sector	93
Funds / Banking sector	28
Insurance sector	58
Consultants / Auditors	35
Admin. and company domiciliation	17
Law firms	8
SFP	48
Asset management	22
Other	14
Total number:	545

Active members 440
Honorary members 105

Total number: 545

Meetings and activities:

Monthly	Board meetings
1 / 2 x per year	Plenary assemblies
2 / 3 x per year	Informal meetings on a subject

– **Conseil d'administration:**

Jean-Noël LEQUEUE	Président
Claudine FRUTSAERT	Vice-Président, section assurances
Patrick WATELET	Vice-Président, section fonds
Vincent SALZINGER	Vice-Président, section banques
Marie-Hélène CLAUDE	Trésorière
Guillaume BEGUE	Administrateur
Sundhevy GOÏOT	Administrateur
Jean-Marie LEGENDRE	Administrateur, Président honoraire
Custodio PORTASIO	Administrateur
Thierry GROSJEAN	Administrateur
Patrick SCHOTT	Administrateur
Olivier GILSON	Conseiller
Patrick CHILLET	Conseiller
Tim WINFIELD	Conseiller
Karine VILRET-HUOT	Conseiller
Benoît MARTIN	Conseiller
Rob Sonnenschein	Conseiller

– **Secrétariat de l'ALCO:**

Emilie Schmitt
secretariat@alco.lu
2 rue de l'Eau
L-1449 Luxembourg
Tél: 26-63-86-25

– **Secrétariat du Bulletin:**

Emilie Schmitt
secretariat@alco.lu

– **Comité de rédaction:**

Claudine FRUTSAERT (responsable), Patrick SCHOTT, Jean-Marie LEGENDRE, Julie BECKER, Leen BOM, Stefano PIERANTOZZI, Olivier GILSON, Jean-François PEMMERS, Sandra SIMON, Ingrid MALMEDY, Sundhevy GOÏOT, Karine VILRET-HUOT, Jean Noël LEQUEUE, les membres du GT 33 et du GT34